IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MISSOURI EASTERN DIVISION

JILL ADAMS, individually and on behalf of all others similarly situated, Plaintiff, v. PSP GROUP, LLC d/b/a PET SUPPLIES PLUS, Defendant.	Case No.: 4:22-cv-1210-RLW

DEFENDANT PSP GROUP, LLC'S MEMORANDUM IN SUPPORT OF MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT

INTRODUCTION

Plaintiff is an aspiring serial class representative who has jumped on the bandwagon of "session replay" wiretapping litigation. Her claim in this case—like her simultaneous case against Zillow—is that the pet supply website operated by PSP Group, LLC ("PSP") is a criminal instrument of mass-wiretapping. Violation of the federal and Missouri wiretapping statutes is punishable by four or five years in prison, respectively. *See* Missouri Wiretapping Act, Mo. Rev. Stat. §§ 542.400–.425 ("MWA"); Electronic Communications Privacy Act, 18 U.S.C.S. §§ 2510–2523 ("ECPA"); Mo. Rev. Stat. § 558.011.1(5). According to ECF No. 27, Plaintiff's First Amended Class Action Complaint ("FAC"), Plaintiff visited www.petsuppliesplus.com for the purpose of finding a local PSP store. The FAC does not identify any more specifics of Plaintiff's experience, but generally argues that the data she transmitted to the website was "intercepted." On the face of the FAC, these "intercepted" transmissions consisted of the fact that a visitor navigated to the PSP website, searched for a store, and any incidental clicks or mouse movements. Courts adjudicating similar Internet-related class claims over the last 20 years have routinely rejected Plaintiff's construction of the wiretapping laws. It misconstrues the statutes' text, criminalizes the ordinary operation of the Internet in ways no legislature intended, and—with respect to the MWA—unconstitutionally burdens interstate commerce. Basic fair notice principles and the rule of lenity require legislatures to give far clearer notice before subjecting "*every website*" to criminal prosecution for using commonplace tools to understand how people use the site.[1] The MWA and the ECPA do not apply; even if they did, *PSP is not guilty of "wiretapping" because neither statute prohibits a party from recording its own conversations.*

[1] *See* FAC at ¶ 27 n.17 (incorporating and relying upon a 2020 Internet article, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*).

Plaintiff's amended pleading does not shore up the fundamental flaws in her state and federal wiretapping claims, and her nine other attempts to state a claim likewise fail on their merits. But the Court need not reach the merits as the FAC should be dismissed in its entirety for three reasons: First, the FAC lacks specific allegations showing that Plaintiff suffered an actual, concrete injury during her limited use of the website. Plaintiff's inability to show harm falls short of the injury-in-fact showing she is required to make under Article III of the Constitution and deprives this Court of subject matter jurisdiction. Second, this Court lacks personal jurisdiction over PSP, because its website does not specifically target Missouri residents. Third, while Plaintiff claims PSP's website "recorded" her activity without notice or consent, the PSP Privacy Policy provides clear notice of PSP's use of anonymous website analytics tools like session replay.

Both Plaintiff's pleadings have elided over Plaintiff's uneventful experience with dozens of pages of hypothetical, generalized discussion of session replay software. But conjecture and others' anecdotes do not state a claim for this plaintiff. Plaintiff must plausibly, concretely allege facts about a specific encounter she had with a specific defendant. The original Complaint failed to describe her experience at all, and now, with the benefit of amendment, ***Plaintiff shows that her experience on the PSP website was brief, unremarkable, and non-injurious***: she went to PSP's website to search for a local store where she later bought birdseed. She now claims that information she shared with PSP was recorded illegally and without her knowledge or consent, but identifies no private or sensitive information or resulting harm. The FAC does not cure Plaintiff's deficient jurisdictional allegations or state a claim. Accordingly, the Court should dismiss this matter with prejudice.

STATEMENT OF RELEVANT FACTS

PSP is a retailer of pet supplies organized as a limited liability company under Delaware law with a principal place of business in Michigan. FAC at ¶ 6. PSP operates the website

www.petsuppliesplus.com, where visitors can find products and locate stores. *Id.* at ¶¶ 11. Plaintiff alleges that there are PSP-affiliated stores within the state of Missouri. *Id.*.

Plaintiff is a Missouri citizen who claims that she accessed PSP's website from Missouri. *Id.* at ¶¶ 5, 63. Beyond briefly visiting the site to search for a local store, Plaintiff identifies no particulars of her website experience, such as products viewed, objects placed in a shopping cart, purchases, filled-out text fields, or messages directed to PSP. *Id.* at ¶¶ 64-68. She admits that she "did not end up purchasing any products on her visit to [the PSP website]." *Id.* at ¶ 67. Plaintiff claims that the site embeds snippets of JavaScript code defined as "Session Replay Code" on visitors' browsers to track certain "mouse or finger movements, clicks, keystrokes . . . URLs of web pages visited, and/or other electronic communications," all of which the FAC defines as "Website Communications." *Id.* at ¶ 1.

Plaintiff made substantively the same generic website browsing allegations against Zillow. *Compare* ECF No. 27, FAC at ¶¶ 1-2 *with Adams v. Zillow Group, Inc.*, Case No. 4:22-cv-1023 (E.D. Mo. 2022), ECF No. 1, Compl. at ¶¶ 1-2 (containing the same language, almost word-for-word). Upon amendment, the FAC now specifies that sometime following her website visit to locate a PSP store, Plaintiff made an in-person purchase of birdseed at the store. FAC at ¶¶ 67, 175-176.

The FAC claims PSP uses session replay software that gathers data on website visitors without prior notice or consent. *Id.* at ¶¶ 2, 68, 86-91, 109-122. In doing so, Plaintiff relies on and characterizes PSP's website, Privacy Policy, and Terms of Use. *Id.* at ¶¶ 90-92, 117-124. [2]

[2] Because she omits these necessary portions of her pleading, they are attached hereto as **Exhibit 1** (Pet Supplies Plus Privacy Policy) and **Exhibit 2** (PSP Terms of Use). Materials necessarily embraced by the pleadings or whose contents are alleged may be deemed incorporated by reference. *Mattes v. ABC Plastics, Inc.*, 323 F.3d 695, 697 n.4 (8th Cir. 2003).

The FAC includes screen-captured images that depict ***purely anonymous*** transmission of data consistent with the Privacy Policy. *Id.* at ¶¶ 74-75; *and see* Exhibit 1.

Plaintiff does not identify any injury in fact that occurred through her use of the PSP website or as a result of PSP's receipt of anonymous website activity data that she directed to PSP. Though she complains that session replay may capture or "compel" transmission of content she entered into text boxes but did not intend to send, she does not allege that she filled out any text boxes on the website. Nor does she identify information that she entered but did not wish to transmit. She also does not deny that she sent information to the website by intentionally interacting with it – in fact, her claims of "wiretapping" are based on the theory that these were intentional communications with PSP. Instead, Plaintiff recites a litany of non-specific, hypothetical, often abstract conjectural harms, such as "diminished value" and deprivation of "economic value" of website "interactions" that she never attempted to monetize or sell and does not value (FAC at ¶¶ 194, 208, 222), unspecified "interference" with personal computers, devices, and data (¶¶ 219, 223, 227-229, 240), hypothetical "compelled" disclosures of unidentified information (*id.* at ¶¶ 34-36, 155, 204, 254, 269, 284, 292), "exposure" to possible future injury (*id.* at ¶ 231), and resulting emotional distress. *Id.* ¶¶ 206-207.

LEGAL STANDARD

Federal courts lack subject matter jurisdiction if a plaintiff lacks standing, which requires an injury in fact that is concrete, real, and not abstract. *See Faibisch v. Univ. of Minn.*, 304 F.3d 797, 801 (8th Cir. 2002); *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) (requiring plaintiff to plead an injury that is "concrete," "real, and not abstract" (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)). To meet the threshold constitutional standing requirement, Plaintiff must show she "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."

Spokeo, 578 U.S. at 338, 340 ("A 'concrete' injury . . . must actually exist."). To defeat a motion under Rule 12(b)(1), Plaintiff "must 'clearly . . . allege facts demonstrating' each element." *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

To defeat a motion for lack of personal jurisdiction under Rule 12(b)(2), the nonmoving party is required to make a prima facie showing of jurisdiction based on the pleadings, affidavits, and exhibits. *J.H. Berra Paving Co. v. Legendary Motorcar Co.,* No. 18-CV-02148, 2019 U.S. Dist. LEXIS 92248, at *1-2 (E.D. Mo. June 3, 2019) (dismissing a Missouri Merchandising Practices Act ("MMPA") claim for lack of personal jurisdiction).

Under Rule 12(b)(6), only complaints that "state[] a plausible claim for relief survive[] a motion to dismiss." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). And although material allegations of fact are accepted as true, factual inferences are resolved in Plaintiff's favor, bald assertions or inferences of fact, as well as "threadbare" legal conclusions couched as factual allegations, must be rejected. *See id.* at 678; *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007).

LEGAL ARGUMENTS AND AUTHORITIES

I. PLAINTIFF LACKS ARTICLE III STANDING BECAUSE AT MOST SHE ALLEGES HYPOTHETICAL INJURIES THAT DO NOT REPRESENT HER OWN EXPERIENCE ON THE PSP WEBSITE

As courts of limited jurisdiction, federal courts "do not adjudicate hypothetical or abstract disputes" nor do they "possess a roving commission to publicly opine on every legal question." *TransUnion*, 141 S. Ct. at 2203. To invoke this court's subject matter jurisdiction, Plaintiff must show that she suffered an actual, concrete injury. *See Spokeo,* 578 U.S. at 338-40. "Article III standing requires a concrete injury even in the context of [an alleged] statutory violation." *TransUnion*, 141 S. Ct. at 2198 (quoting *Spokeo*, 578 U.S. at 341). Moreover, a plaintiff cannot rely on "attenuated chain[s] of inferences" or "speculation." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414-15 n.5 (2013); *see also TransUnion,* 141 S. Ct. at 2211-12.

Plaintiff has not shown any "concrete" injury. *See Spokeo,* 578 U.S. at 340 ("A 'concrete' injury must be '*de facto*'; that is, it must actually exist. When we have used the adjective 'concrete,' we have meant to convey the usual meaning of the term—'real,' and not 'abstract.'" (citations omitted)). In attempting to plead an injury-in-fact, Plaintiff alleges generally that she "fell victim to [PSP's] unlawful monitoring" of her "Website Communications." FAC at ¶¶ 1, 64, 71, 72. She claims that PSP diminished and/or deprived her of the value of this information (namely, the fact that she visited the site, that she used the site's store locator, and the clicks and keystrokes incidental to that activity). *Id.* at ¶¶ 194, 208, 222. Without factual explanation, she recites a number of further conclusory allegations: PSP wrongfully detained and interfered with her personal computers, devices, or data (¶¶ 219, 223, 227-229, 240), exposed her to possible future injury (¶ 231), caused her emotional distress (¶¶ 206-207), and "compelled" her to disclose information that she would not have chosen to transmit. FAC at ¶¶ 34-36, 154, 269, 284, 292.

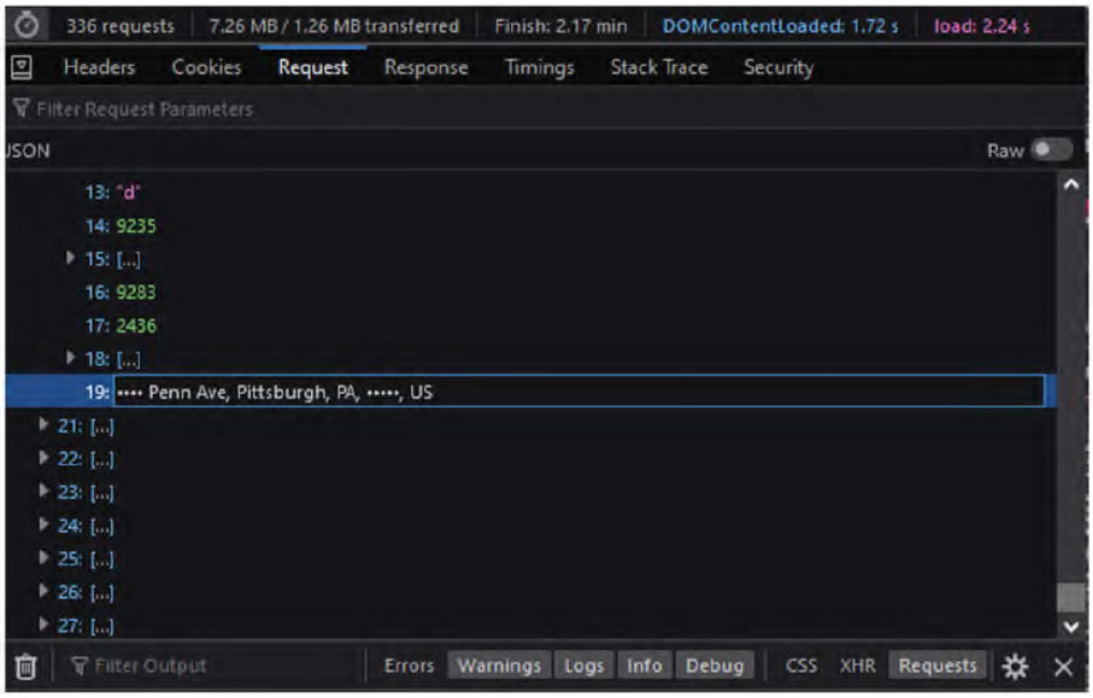
The allegation that the PSP website ***may*** capture text entered in "form fields" that Plaintiff did not choose to submit is typical of the FAC's failure to plead "facts arising out of a specific encounter with a specific defendant." *Byars v. Hot Topic, Inc.*, No. EDCV 22-1652, 2023 U.S. Dist. LEXIS 24985, at *9, *11 (C.D. Cal. Feb. 14, 2023) (raising *sua sponte* serial plaintiff's failure to establish subject matter jurisdiction in similar website "wiretapping" case). The FAC does not identify a single example of text Plaintiff entered but did not intend to transmit. The only factual claim about her use of the website is that she searched for a local PSP store.[3]

Plaintiff also does not explain how PSP "interfered" with her right to possess, use, or control any computers, mobile devices, or data. Counts IV, V, and VI contain naked recitals of

[3] *See* **Exhibit 4** (PSP Store Locator). The Locator tool uses anonymous zip code or city/state-level data entered by the user to display a list of nearby stores.

the elements of claims for trespass, conversion, or replevin. FAC at ¶¶ 212-243. But far from showing an injury in fact, the FAC never explains how Plaintiff's fleeting website visit resulted in even *de minimis* dispossession of (or harm to) anything belonging to her. *See In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 930-33 (N.D. Cal. 2015) (dismissing trespass, conversion, and privacy tort claims for failure to show "concrete and particularized harm").

Plaintiff's intercepted "Website Communications," as she defines them, do not consist of anything to which a right of privacy attaches. *See Massie v. GM LLC*, Civ. Act. No. 21-787, 2022 U.S. Dist. LEXIS 28969, at *13-14 (D. Del. Feb. 17, 2022) (allegation that session replay code collected anonymized, non-personal data in which plaintiff had no recognized privacy interest failed to establish standing). Although Plaintiff applies conclusory labels like "private," "personally identifiable," "personal," "personalized," and "sensitive" (FAC at ¶¶ 99, 231, 317-18), the FAC describes one brief website visit. At most, the site captured "what content was being viewed, clicked on, requested, and/or input by Plaintiff." FAC at ¶¶ 69, 100. And the FAC does not deny that this was collected ***anonymously***—that is, in a way that avoids identifying individuals.



FAC at ¶¶ 37, 75, 80. Contrary to Plaintiff's contention that this picture shows "captured" addresses being "sent to" Microsoft, it demonstrates that the street number and zip code have been deliberately withheld. The Privacy Policy confirms that "information that is automatically submitted to us by your computer or device is considered anonymous information. To the extent we share such information with third parties, it is not traceable to any particular user." *See* Exhibit 1. The information received by PSP is not private and is no different than the information any attentive retailer would receive if they were listening when a shopper spoke to them.

Plaintiff's allegation that "her" data was recorded and may be accessed by third parties is the sort of indefinite, conjectural claim that this Court and others routinely reject. *See Duqum v. Scottrade, Inc.,* No. 15-CV-1537, 2016 U.S. Dist. LEXIS 89992, at *27-31 (E.D. Mo. July 12, 2016) (dismissing putative class action for lack of Article III standing where plaintiffs alleged diminution in value of their personal information, loss of privacy, and increased risk of future harm following a data breach); *see also Massie*, 2022 U.S. Dist. LEXIS 28969, at *12 (dismissing for lack of standing a session replay lawsuit because "'[e]avesdropping' on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury.").

Plaintiff's suggestion that PSP diminished the value of her anonymous website interactions is conjectural and unsupported by any pleaded facts. *See In re Facebook,* 140 F. Supp. 3d at 931-32 ("Plaintiffs have not shown, for the purposes of Article III standing, that they personally lost the opportunity to sell their information or that the value of their information was somehow diminished"); *Del Vecchio v. Amazon.com Inc*., No. C11-366, 2011 U.S. Dist. LEXIS 138314, at *10, *24 (W.D. Wash. Nov. 30, 2011) (finding the allegation that defendant "deprived [Plaintiffs] of the opportunity to exchange their valuable information" to be entirely speculative and

dismissing for failure to "plead adequate facts to establish any plausible harm" (alteration in original) (internal quotation marks omitted)). Raw data about one individual on a single website has *de minimis* value at best, but whatever the theoretical value of website browsing data about Plaintiff, the FAC does not show that Plaintiff ascribed value to it or tried to monetize or otherwise capture that value for herself.[4]

The FAC should be dismissed with prejudice because it fails to show that Plaintiff has standing, and this Court consequently lacks subject matter jurisdiction over Plaintiff's claims.

II. THE COURT LACKS SPECIFIC JURISDICTION OVER PSP WHERE HER CLAIMS ARISE EXCLUSIVELY FROM A WEBSITE THAT DOES NOT TARGET MISSOURI

The Court lacks personal jurisdiction over PSP and should dismiss the FAC. In her amended pleading, Plaintiff alleges that PSP is a Delaware limited liability company with a principal place of business in Michigan. FAC at ¶¶ 6-7. She does not argue that PSP is "at home" in Missouri such that this Court may hear any claim against it. *See Viasystems, Inc. v. EBM-Papst St. Georgen GmbH & Co., KG*, 646 F.3d 589, 595 (8th Cir. 2011) ("[T]he paradigm forum" is where "the corporation is fairly regarded as at home." (internal quotation marks and citation omitted)). This Court lacks general jurisdiction over PSP.

The Court also lacks specific jurisdiction over these claims. Missouri's long-arm statute is coextensive with the Due Process Clause of the United States Constitution. *Institutional Food Mktg. Assocs., Ltd. v. Golden State Strawberries, Inc.*, 747 F.2d 448, 453 (8th Cir. 1984). To

[4] *See Vecchio v. Amazon.com, Inc.*, No. C11-366, 2012 U.S. Dist. LEXIS 76536 (W.D. Wash. June 1, 2012) ("It is not enough to allege only that the information has value to Defendant; the term 'loss' requires that Plaintiffs suffer a detriment . . . ."); *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592, 2016 U.S. Dist. LEXIS 112315, at *18 (S.D.N.Y. Aug. 17, 2016) ("[B]rowsing information may possess value in the abstract, [but] absent allegations suggesting that plaintiffs' ability to monetize their browsing information was diminished, this alleged harm remains too conjectural.").

establish specific jurisdiction, Plaintiff must allege facts showing that PSP has constitutionally sufficient "minimum contacts" with Missouri such that it could reasonably anticipate being haled into court there. *See J.H. Berra*, 2019 U.S. Dist. LEXIS 92248, at *8-9 (citing *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980)). The five factors analyzed to determine whether a defendant has sufficient minimum contacts are: "(1) the nature and quality of contacts with the forum state; (2) the quantity of the contacts; (3) the relation to the cause of action to the contacts; (4) the interest of the forum state in providing a forum for its residents; and (5) convenience of the parties." *J.H. Berra*, 2019 U.S. Dist. LEXIS 92248, at *9 (citation omitted). The first three factors are "primary," though the totality of the circumstances is considered. *Id*.

Even with the benefit of amendment, the FAC does not allege facts that would show PSP has sufficient minimum contacts with Missouri. In successive pleadings, Plaintiff has repeated the same conclusions. FAC at ¶¶ 10-13. Plaintiff now adds additional conclusory recitations that do nothing to confer jurisdiction. *Id.* ¶¶ 11, 13-14. The FAC also adds some facts, but to no avail. The Complaint alleged that PSP offers a website it knows is available in Missouri. *See* ECF No. 1. at ¶ 11. The FAC now adds that PSP has brick-and-mortar stores in Missouri and ships products to Missouri that are purchased through its website. FAC at ¶¶ 10-12.

Neither of these allegations confers specific jurisdiction *in this case*. PSP's brick-and-mortar presence and e-commerce capabilities do not confer personal jurisdiction as to Plaintiff's claims. *See Steinbuch v. Cutler*, 518 F.3d 580, 586 (8th Cir. 2008) (specific jurisdiction exists where a plaintiff's claims arise from or relate to defendant's forum activities). Plaintiff's claims arise from the collection of data on PSP's website—in-state stores and online ordering are immaterial red herrings. "[E]ven regularly occurring sales of a product in a state do not justify the exercise of [specific] jurisdiction over a claim unrelated to those sales." *Allied Ins. Co. of Am. v.*

JPAULJONES L.P., 491 F. Supp. 3d 472, 475 (E.D. Mo. Sept. 29, 2020) (alteration in original) (quoting *Bristol-Myers Squibb Co. v. Super. Ct. of Cal., S.F. Cnty.*, 137 S. Ct. 1773, 1781 (2017)). Had Plaintiff ordered a product for pick-up in a store or alleged a tortious injury on the premises, there might be some nexus to *that* store. Had she placed an online order, there might be specific jurisdiction over *that* transaction. But specific (as opposed to general) jurisdiction does not emanate generally from the presence of multiple contacts; for specific jurisdiction, due process requires Plaintiff to show that *her specific* claims arise from specific forum contacts. *See Fidrych v. Marriott Int'l, Inc.*, 952 F.3d 124, 140-42 (4th Cir. 2020) (dismissing a lawsuit by a South Carolina resident for lack of personal jurisdiction where Marriott did business in-state and plaintiff reviewed Marriott's website to learn about the Italian hotel where his personal injury occurred).

With respect to the website from which her claims arise, Plaintiff cannot show that the PSP website intentionally "targets" Missouri. Maintaining a public website accessible from many locations does not mean that each of those locations is targeted. *See Johnson v. Arden*, 614 F.3d 785, 796 (8th Cir. 2010) (a "website's accessibility in Missouri alone is insufficient"); *Allied Ins. Co. of Am.*, 491 F. Supp. 3d at 477-78 (dismissing claim for lack of specific jurisdiction and "join[ing] with many others in holding that specific jurisdiction does not attach simply because a defendant operates a commercial website that is, at some level, interactive and allow[s] for sales into the forum state."). The FAC does not identify any feature of the website directed to Missouri.[5] "We need not belabor the point: if having an interactive website were enough in situations like this one, there is no limiting principle—a plaintiff could sue everywhere." *Advanced Tactical*

[5] The Court may take judicial notice of contents of a website to decide personal jurisdiction. *See Enterprise Rent-A-Car Co. v. U-Haul Int'l, Inc.*, 327 F. Supp. 2d 1032, 1042 n.4 (E.D. Mo. 2004).

Ordinance Sys., LLC v. Real Action Paintball, Inc., 751 F.3d 796, 803 (7th Cir. 2014); *see also Allied Ins. Co. of Am.*, 491 F. Supp. 3d at 475-77 (quoting same and adopting *Fidrych*, *supra*).

III. PLAINTIFF IS A SAVVY SERIAL LITIGANT WHO HAD AMPLE NOTICE OF PSP'S PRIVACY POLICY AND CONSENTED TO ITS TERMS

If anyone should be expected to read a website privacy policy, it is this Plaintiff. Weeks before filing this suit, Plaintiff claimed to suffer the same "mental anguish, emotional distress, worry, [and] fear" as a result of Zillow's use of session replay on its website. *See Adams v. Zillow Group, Inc.*, No. 4:22-CV-1023 (E.D. Mo. 2022), Compl. at ¶ 120. A reasonable person who purports to be highly offended by session replay cannot forever profess that she is "shocked, shocked!" to find this software in use on each website she chooses to sue. All site visitors have abundant notice of PSP's website data collection practices. A link to the Privacy Policy is featured under a bold, all-caps "**TERMS & PRIVACY**" header. *See* **Exhibit 3**. This "**TERMS & PRIVACY**" section remains conspicuous on each page of the website. The Privacy Policy begins:

Pet Supplies Plus® Privacy Policy

Updated September 15, 2020

This Privacy Policy ("Policy") applies to PSP Group, LLC its affiliates, subsidiaries, divisions and designees. ("Pet Supplies Plus" or "we"). This Policy describes how Pet Supplies Plus collects, shares, uses, and safeguards customer personal information ("Personal Information"). This Policy covers Personal Information we collect anywhere. This includes our Pet Supplies Plus retail stores, our websites at Pet Supplies Plus.com, and any other websites where we post this Policy (collectively the "Site").

INFORMATION WE COLLECT

We may automatically collect some information when you come to our Site. This information helps us improve our Site and your experience on our Site.

Automatic Anonymous Information

What we collect automatically includes information about the computer or device you use to come to our Site. This may include the software that runs your computer, the type of software you use to access and search the internet, the service you use to go online, and the internet address assigned to your computer. This information helps us make our Site work better with your systems. We also collect data about how you use our Site such as the times you come to our Site and for how long. We may also know what websites you went to before and after our Site. It is not uncommon for online stores to collect this type of data. The information that is automatically submitted to us by your computer or device is considered anonymous information. To the extent we share such information with third parties, it is not traceable to any particular user and will not be used to contact you.

The succeeding sections elaborate on the collection of "Automatic Anonymous Information" through third-party vendor-supplied analytics, cookies, pixel tags, and the like. *See* Exhibit 1. Collection and use of non-anonymous data—actual personal information—is also described. *Id.*

Every PSP website visitor—and this veteran class representative, in particular—is on notice that PSP automatically collects and anonymously shares data about visitors' use of the site. *Id.* All of Plaintiff's claims are predicated on the absence of notice and/or consent to data collection practices that are clearly described in the privacy policy. Each claim should therefore be dismissed for failure to state a claim. *See Silver v. Stripe, Inc.,* No. 20-CV-08196, 2021 U.S. Dist. LEXIS 141090, at *10-11 (N.D. Cal. July 28, 2021) (dismissing class wiretapping claims based on finding that plaintiffs consented to privacy policy); *Jacome v. Spirit Airlines*, 2021 Fla. Cir. Lexis 1435, at *20-22 (11th Cir. Ct. June 17, 2021) (holding that privacy policy put plaintiff on "inquiry notice" that the site tracked "mouse clicks and movements" and "information inputted" by her when browsing the airline website).

IV. PLAINTIFF'S INTRUSION UPON SECLUSION CLAIM FAILS BECAUSE ANALYZING ONE'S OWN WEBSITE TRAFFIC DOES NOT VIOLATE VISITORS' PRIVACY RIGHTS AND IS NOT HIGHLY OFFENSIVE (COUNT III)

Browsing and searching the Internet is like traveling along a public highway and "leaving the equivalent of a calling card at each website visited." *U.S. v. Taylor*, 935 F.3d 1279, 1285 n.4 (11th Cir. 2019) (discussing reasonable expectation of privacy in online "movements" under the Fourth Amendment). Any expectation of privacy, however sincerely Plaintiff felt it, was not reasonable: when Plaintiff navigates to a public website, she has no right to expect that the site will not record and use data about how she used the site. Holding otherwise would mean that virtually every visit to every website from anywhere creates a potential cause of action.

Plaintiff's intrusion upon seclusion claim fails as a matter of law because she has not demonstrated "(1) the existence of a secret and private subject matter; (2) a right in the plaintiff to

keep that subject matter private; and (3) the obtaining by the defendant of information about that subject matter through unreasonable means." *Tesar v. Union R-Xi Sch. Dist.*, No. 15CV943, 2017 U.S. Dist. LEXIS 20399, at *16-17 (E.D. Mo. Feb. 9, 2017) (citations omitted) (dismissing intrusion claim for failure to state a claim). Intrusion upon seclusion is an "intrusion 'physically or otherwise upon the solitude or seclusion of another or his private affairs or concerns' in a manner that would be 'highly offensive to a reasonable person.'" *Id.* at *16 (quoting *Sofka v. Thal*, 662 S.W.2d 502, 510 (Mo. 1983)). In the Internet privacy litigation context, such claims routinely fail because:

> websites routinely embed content from third-party servers in the form of videos, images, and other media, as well as through their use of analytics tools, advertising networks, code libraries and other utilities. Each tool transmits to third parties the same data that Plaintiffs claim is highly sensitive. Since these requests are part of routine internet functionality and can be easily blocked, the Court finds that they are not a "highly offensive" invasion of Plaintiffs' privacy interests.

In re Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 846-47 (N.D. Cal. 2017) (collecting cases dismissing intrusion upon seclusion claims); *see also In re Vizio, Inc.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) ("Courts have been hesitant to extend the tort of invasion of privacy to the routine collection of personally identifiable information.").

The FAC, like the Complaint, fails to plead the existence of any secret and private subject matter in which Plaintiff had a recognized privacy right. In the FAC, Plaintiff alleges that PSP "required Plaintiff to disclose that which she chose not to communicate as well as what she chose to send, which is highly offensive." FAC at ¶ 204. As discussed above at Section I, the FAC never identifies "that" which she chose not to communicate: Plaintiff points to no text boxes that she filled or information she entered but did not wish to transmit. In any event, visitors to a website do not have a recognized privacy right in their voluntary interactions with the site. *Massie*, 2022 U.S. Dist. LEXIS 28969, at *12 ("Plaintiffs do not have a reasonable expectation of privacy over

the anonymized data captured by the Session Replay software at issue here."); *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321 (S.D. Fla. Sept. 9, 2021) ("[M]ere tracking of Plaintiff's movements on Defendant's website is the cyber analog to record[ing] information Defendant could have obtained through a security camera at a brick-and-mortar store").

The FAC also fails to show that Plaintiff "conducted . . . herself in a manner consistent with an actual expectation of privacy." *Saleh v. Nike*, 562 F. Supp. 3d 503, 524-25 (C.D. Cal. 2021) (citing *Hill v. NCAA*, 7 Cal. 4th 1, 26 (1994)); *see also* Restatement (Second) of Torts § 652B cmt. c (Am. L. Inst. 1977) (liability arises only where a defendant has "intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs"). There is no allegation that Plaintiff ever sought to protect the privacy of her browsing information, e.g., by using simple tools to block website analytics and cookies. *See In re Facebook*, 263 F. Supp. 3d at 846 (finding alleged intrusion "could have been easily blocked, but [p]laintiffs chose not to do so"). Where Plaintiff already made similar allegations against another website, her failure to protect herself seems inconsistent with any real expectation of privacy.

The FAC also fails to plead "highly offensive" conduct. Plaintiff's allegations do not meet the high bar of showing conduct that would be highly offensive to a reasonable person. *See In re Facebook*, 263 F. Supp. 3d at 846-47 (collecting cases); *Popa v. Harriet Carter Gifts, Inc.,* 426 F. Supp. 3d 108, 122 (W.D. Pa. 2019) (holding that use of session replay software is "simply not the type of highly offensive act to which liability [for intrusion upon seclusion] can attach."), *aff'd in relevant part, rev'd on other grounds*, 52 F.4th 121 (3rd Cir. 2022). The bare allegations that Plaintiff suffered "mental anguish" and "emotional distress" and that "PSP's conduct is highly objectionable" (FAC ¶¶ 205-207) are not sufficient. *Tesar*, 2017 U.S. Dist. LEXIS 20399, at *16 (holding that mere allegations that "[d]efendants improperly intruded upon her protected records"

were insufficient to state a plausible claim for intrusion upon seclusion). Count III fails to state a claim and should be dismissed with prejudice.

V. PLAINTIFF FAILS TO STATE A WIRETAPPING CLAIM UNDER BOTH THE MISSOURI AND FEDERAL WIRETAPPING STATUTES (COUNTS I & VII)

Counts I and VII should be dismissed because a party is not prohibited from recording its own "communications" under either Missouri's MWA and the federal ECPA, which are one-party consent statutes. Even more fundamentally, neither the ECPA nor the MWA applies to the use of session replay code or similar website analytics technology: the MWA does not apply to electronic communications at all. And while the ECPA was revised in the 1980s to apply to the Internet, it has nothing to say about websites' interpretation and analysis of visitors' voluntary site traffic.

A. PSP Did Not Wiretap Itself

The ECPA and MWA are one-party consent statutes. Only one party need consent to a recording under the MWA, Mo. Rev. Stat. § 542.402.2(3), and under the ECPA, 18 U.S.C.S. § 2511(2)(d). This largely bars website "wiretapping" claims where the website operator is accused of ***both*** receiving ***and*** wiretapping the same communications. *See Allen v. Quicken Loans, Inc.*, Civ. Act. No. 17-12352, 2018 U.S. Dist. LEXIS 192066, at *12 (D.N.J. Nov. 9, 2018) ("[T]he ECPA is a one-party consent statute, and so long as 'one of the parties to the communication has given prior consent to such interception,' no liability exists . . . ." (citations omitted)).

The FAC admits everything needed for dismissal of Counts I and VII. Plaintiff alleges that she directed "communications" to PSP, who received and responded to them. *See* FAC at ¶¶ 1, 49, 70, 71, 96, 101, 105-106, 154, 160. She alleges that PSP intercepted and recorded these same communications. *Id.* at ¶¶ 50, 96, 97, 101, 153, 160, 253. She thus pleads herself out of a claim. *Jurgens v. Build.com, Inc.*, No. 17-CV-00783, 2017 U.S. Dist. LEXIS 186999, at *13-15 (E.D. Mo. Nov. 13, 2017) (dismissing website wiretapping claim where, "[a]s a party to the

communication, Defendant is exempt from liability under the [ECPA]").

The crime-tort exception requires pleading of an independent tortious or criminal motive for the act of recording. To evade the one-party consent rule, Plaintiff argues that PSP intercepted her communications "for the purpose of committing [a] criminal or tortious act." MWA, Mo. Rev. Stat. § 542.402.2(3); ECPA, 18 U.S.C.S. § 2511(2)(d). Specifically, Plaintiff asserts that PSP intended to invade her privacy, to intrude upon her seclusion, and to violate the MMPA. FAC ¶¶ 163, 264. This fails to state a claim. *Iqbal*, 556 U.S. at 678 (labels, conclusions, formulaic recitations, and naked assertions devoid of "further factual enhancement" fail to state a claim (citing *Twombly*, 550 U.S. at 556-57).

The crime-tort exception only applies where Plaintiff has shown that tortious or criminal intent existed "independent of the act of recording itself." *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010). "[T]he tort cannot be the act of interception." *Cohen v. Casper Sleep Inc.*, No. 17cv9325, 17cv9389, 17cv9391, 2018 U.S. Dist. LEXIS 116372, at *11 (S.D.N.Y. July 12, 2018) (citing *Caro*, 618 F.3d at 100); *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971) ("[T]he sort of conduct contemplated [by Congress] was an interception by a party to a conversation with an intent to use that interception against the non-consenting party in some harmful way and in a manner in which the offending party had no right to proceed."). This is essentially a *mens rea* requirement. *See In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 514-19 (S.D.N.Y. Mar. 28, 2001) (dismissing similar website "wiretapping" claims and collecting authorities). The FAC fails to show that PSP deployed session replay ***for the purpose*** of committing an independent criminal or tortious act; *e.g.*, blackmail or theft of trade secrets. *Caro*, 618 F.3d at 98-100 (collecting cases); *Jurgens*, 2017 U.S. Dist. LEXIS 186999, at *13 n.4 (*citing Caro* at 100-101).

Far from demonstrating an independent, tortious purpose, the FAC contends that "the only

purpose" for "Defendant's use of Session Replay Code" "was to gain an unlawful understanding of the habits and preferences of users to its website, and the information collected was solely for Defendant's own benefit" to "be used to market Defendant's services and goods to Plaintiff and the Class Members." FAC ¶¶ 124-125. If true, this "only purpose" of serving ads and selling goods is self-evidently non-tortious and non-criminal. For decades, courts have agreed that "the tort or crime exception cannot apply where the interceptor's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'" *In re Google Inc. Gmail Litig.*, No. 13-MD-02430, 2014 U.S. Dist. LEXIS 36957, at *69-70 n.13 (N.D. Cal. Mar. 18, 2014) (quoting *In re Doubleclick*, 154 F. Supp. 2d at 519). Plaintiff's admissions eviscerate her claims.

B. The MWA Does Not Apply to Electronic Communications

Plaintiff ignores the MWA's narrow scope. Plaintiff baldly represents that her interaction with PSP's website "is electronic communications [sic] under the Missouri Wiretap Act." FAC at ¶ 70. This overlooks that the Missouri Wiretapping Act does not define, mention, or contemplate "electronic communications" of any kind.[6] PSP's initial memorandum in support identified this inconsistency, but the FAC continues to ignore the MWA's scope, history, text, and intent.

The "Missouri law, unlike the federal statute, applies only to 'wire communications.'" *Angel. v. Williams*, No. 92-5084-CV-SW-1, 1993 U.S. Dist. LEXIS 19003, at *4-5 (W.D. Mo. Jan. 11, 1993) (dismissing "wiretapping" claims by three Webb City police officers who were recorded allegedly abusing an inmate in the city jail). This was a conscious drafting decision by the Missouri General Assembly. The MWA was enacted in 1989 based on the Federal Wiretap Act (the ECPA

[6] Plaintiff makes the equally erroneous, equally unsupported contention that "[t]he purpose of the Missouri Wiretapping Act is . . . to prevent the pernicious effect on browsers who would otherwise feel insecure from intrusion into their browsing activity." *See* FAC at ¶ 127. Internet "browsing" was in its infancy when the MWA was enacted, and the MWA does not mention the Internet.

predecessor statute), 18 U.S.C.S. § 2510 *et seq*.; *State v. King*, 873 S.W.2d 905, 908 (Mo. Ct. App. 1994). Three years earlier, relevant portions of the Federal Wiretap Act were amended and expanded into the ECPA in order to "extend to 'electronic communications' many of the protections afforded 'wire communications' under the original Wiretap Act." *U.S. v. Ropp*, 347 F. Supp. 2d 831, 834 (C.D. Cal. 2004); *see also* H.R. Rep. No. 99-647 (1986), at 34; *Jurgens*, 2017 U.S. Dist. LEXIS 186999, at *10-11 (summarizing the "post-ECPA Wiretap Act").

Aware of the recently amended ECPA, the General Assembly nevertheless omitted "electronic communications" from its new law and chose operative definitions that covered only auditory communications. A holding that the MWA applies to electronic communications would contradict the intent of the Missouri legislature and upend four decades of legislative scoping decisions and careful drafting by the U.S. Congress and dozens of other state legislatures, as well.

Plaintiff fails to plead an "interception" as defined under the MWA. The MWA definition of "intercept" includes ***only*** "aural acquisition of the contents of any wire communication." *Compare* 18 U.S.C.S. § 2510(4) *with* Mo. Rev. Stat. § 542.400(6). In other words, only things that can be heard can be wiretapped within the meaning of the MWA. "An 'aural acquisition' by definition engages the sense of hearing." *Application of U.S. for Order Authorizing Installation & Use of Pen Register*, 546 F.2d 243, 245 (8th Cir. 1976); *U.S. v. Gregg*, 629 F. Supp. 958, 961 (W.D. Mo. 1986); *see also Carothers v. Carothers*, 977 S.W.2d 287, 290 (Mo. Ct. App. 1998) (interpreting "aural acquisition" as something capable of "later aural disclosure" or "hearing"). The Complaint was devoid of any claims of aural interception. Tellingly, the FAC makes no attempt to shore up this pleading deficiency. None of Plaintiff's allegedly intercepted communications is capable of "auditory acquisition." Nor are they "wire communications" under MWA, § 542.400(12). Count I should be dismissed with prejudice.

C. Plaintiff Fails to Plead Other Basic Elements of "Wiretapping"

Plaintiff fails to allege use of a "device." Plaintiff fails to plead that PSP used an electronic, mechanical, or other device or apparatus to intercept her communications. *See* 18 U.S.C.S. § 2510(4)-(5); Mo. Rev. Stat. § 542.400(5)-(6) (defining "device" and "intercept"). Plaintiff argues that session replay is "***the equivalent of***" a device. FAC ¶¶ 106-107, 152, 251 (emphasis added).[7] Asking the Court to interpret a criminal statute to encompass "equivalents" of defined terms invites grievous error. *See Crandon v. United States*, 494 U.S. 152, 160 (1990) ("Because construction of a criminal statute must be guided by the need for fair warning, it is rare that legislative history or statutory policies will support a construction of a statute broader than that clearly warranted by the text.").

Federal courts have long rejected claims that non-physical, intangible software code is a wiretapping "device." *Potter v. Havlicek*, No. 06-CV-211, 2008 U.S. Dist. LEXIS 122211, at *23 (S.D. Ohio June 23, 2008) (dismissing wiretapping claim because "the word 'device' does not encompass software"); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (finding drives or servers where e-mail is received are not devices). Courts have reached the same ruling regarding session replay. *See Jacome*, 2021 Fla. Cir. LEXIS 1435, at *12-14 (session replay was not a device); *Cardoso v. Whirlpool Corp.,* No. 21-CV-60784, 2021 U.S. Dist. LEXIS 125279, at *6-7 (S.D. Fla. July 6, 2021) (holding same).

Plaintiff's (non-factual) argument that "software" can be a device conflates a website's receipt and processing of information from intentional site users with "spyware" and "keylogger" programs loaded onto computers to record spouse's emails or steal login credentials to perpetrate

[7] The FAC also lists "browsers," "computing devices," and "web-servers" as "devices" at Paragraph 251(a)-(c). None of these is a wiretapping device and none appears related to the facts pleaded in the FAC. Paragraph 251 itself appears to be cut-and-paste from an unrelated action.

identity fraud. *See* FAC ¶¶ 151-152. Public websites are not "devices," and they do not "spy on" site visitors. Courts that have considered this issue have declined to adopt Plaintiff's limitless interpretation of what may constitute a "device." *See, e.g.*, *Jacome*, 2021 Fla. Cir. LEXIS 1435, at *12-14; *Cardoso*, 2021 U.S. Dist. LEXIS 125279, at *6-7.

Plaintiff fails to allege a "communication" or its "contents." Within the meaning of the ECPA, the content of an electronic communication properly refers to "the substantive information conveyed to the recipient," such as "a search phrase entered by a user into a search engine." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 137 (3d Cir. 2015); *see also Graf v. Zynga Game Network, Inc. (In re Zynga Privacy Litig.)*, 750 F.3d 1098, 1105-07 (9th Cir. 2014) ("contents" refer to the "essential part" of a communication, the "meaning conveyed," rather than mere record information like the name and address of the sender). Likewise, "mouse or finger movements, clicks, scrolls, zooms, window resizes, [and] keystrokes" (FAC ¶ 29) facilitate web navigation; they do not reveal contents. *See Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021) (holding that "mouse clicks" and "pages viewed" do not "constitute[] message content in the same way that the words of a text message or an email do"). The *Jacome* court held that such data "do not constitute 'contents' under the Federal Wiretap Act or any of its state analogs because it does not convey the *substance* or *meaning* of any message." *Jacome*, 2021 Fla. Cir. LEXIS 1435, at *7-8, *12; *accord Goldstein v. Luxottica of Am., Inc.*, No. 21-80546-CIV, 2021 U.S. Dist. LEXIS 158935, at *4-5 (S.D. Fla. Aug. 20, 2021), *report and recommendations adopted*, 2021 U.S. Dist. LEXIS 170809 (S.D. Fla. Sept. 8, 2021) (same).

Here, Plaintiff did not communicate or attempt to communicate with anyone, and Congress and the Missouri General Assembly did not criminalize the recording of any data PSP received.

D. The Court Should Avoid Unconstitutional Outcomes and Favor Lenity

The MWA Should Not Be Interpreted to Burden Interstate Commerce. Plaintiff's reading of the MWA would unduly burden interstate commerce. U.S. Const. Art. I., Sec. 8., cl. 3 (granting Congress the power to regulate commerce "among the several States"). As the Supreme Court held in *Pike v. Bruce Church*, 397 U.S. 137 (1970), local and state laws that appear facially neutral may not burden interstate commerce in a way that is clearly excessive in relation to any local benefit. *See id.* at 140-42. Thus, even where the MWA does not appear to discriminate in favor of local interests, its local benefits may not justify an excessive burden placed on interstate commerce. Under Plaintiff's reading of the MWA, it is a violation for a website to record transmissions without prior express consent from the visitor. Such a consent standard would far exceed anything required under federal law, and Missouri would thus dictate a nationwide Internet consent standard: although not required by federal law or by other states, all Internet websites viewable from Missouri (*all websites*) would be required to follow Missouri's new-found heightened consent standard. Non-compliance would subject website operators everywhere to criminal penalties and civil liability. The cost of technical and administrative compliance would be great. By contrast, any putative local benefit "could be promoted as well with a lesser impact on interstate activities." *Id.* at 142. Plaintiff's reading of the MWA fails the *Pike* balancing test and should thus be rejected for the further reason that it would be unconstitutional.

Ambiguous Criminal Statutes Should Be Interpreted in Favor of Lenity. If Plaintiff's interpretations were adopted by the Court, millions would face massive criminal liability under the MWA and the ECPA. *See Cohen*, 2018 U.S. Dist. LEXIS 116372, at *14-15 (observing that if federal wiretapping law covered the recording of website visitors' keystrokes, mouse clicks, and website communications, many website operators would routinely commit felonies); *In re Doubleclick*, 154 F. Supp. 2d at 511-13 (same conclusion as to browser cookies). The rule of

lenity flows from "the fundamental principle that no citizen should be . . . subjected to punishment that is not clearly prescribed." *U.S. v. Parker*, 762 F.3d 801, 806 (8th Cir. 2014) (quoting *U.S. v. Santos*, 553 U.S. 507, 514 (2008)). Were the MWA or the ECPA ambiguous, any ambiguity should be resolved against expanding criminal liability. *See Santos*, 553 U.S. at 513-14.

VI. PLAINTIFF'S OTHER FEDERAL CRIMINAL STATUTORY CLAIMS ALSO FAIL TO STATE A CLAIM (COUNTS VIII, IX, X, & XI)

Plaintiff's other federal computer crimes theories misunderstand both the law and the Internet: that is, "the servers, computers, fiber-optic cables and routers through which data is shared online." *In re Doubleclick*, 154 F. Supp. 2d at 500-02 (summarizing the basic "architecture and engineering" of the Internet). Plaintiff's strained readings of the ECPA, Stored Communications Act ("SCA"), and Computer Fraud and Abuse Act ("CFAA") admit of no limiting principle that avoids casting most website operators as felons. For more than 20 years, courts nationwide have rejected such readings. It is now well established that most commercial websites do not provide "electronic communication services," personal devices are not electronic storage facilities, and nothing prohibits PSP, as the intended recipient, from accessing and disclosing its own communications. ***See Count VIII*** (alleging divulgence of electronic communications in violation of 18 U.S.C.S. § 2511(3)(a)), ***Count IX*** (alleging unauthorized access to an electronic communications storage "facility" under 18 U.S.C.S. § 2701(a)), ***Count X*** (alleging divulgence of electronic communications in violation of 18 U.S.C.S. § 2702(a)).[8]

A. The Prohibitions at 18 U.S.C.S. § 2511(3)(a) (Count VIII) and 18 U.S.C.S. § 2702 (Count X) Do Not Apply to PSP

PSP is not an electronic communication service ("ECS") provider and its website is not an ECS. The relevant prohibitions at ECPA Section 2511(3)(a) (Count VIII) and SCA Section

[8] ***Count XI***, which alleges violation of the CFAA, 18 U.S.C.S. § 1030, is equally meritless.

2702 (Count X) apply only to providers of electronic communication services. In Plaintiff's original pleading, she admitted that "Defendant is not a provider of wire or electronic communication services, or an internet service provider." *See* ECF No. 1, Complaint at ¶ 66. Plaintiff omits that admission from the FAC, but still does not show that PSP is an ECS provider.

PSP is not an ECS provider, and its website is not an ECS. An ECS is a "service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C.S. § 2510(15); *see also In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005) (a company "does not become an [ECS] provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers"); *Crowley*, 166 F. Supp. 2d at 1270 (similar holding).[9]

PSP does not provide any "browser" or "Chrome Service." Without any factual basis or explanation, the FAC refers to Defendant's "**web browser**," storage of content in "**Defendant's browser**," Defendant's "**rendition of the Chrome Service**," and communications with third-party websites and apps. FAC at ¶¶ 268-270, 276-277, 299-300, 308, 310. These allegations are not well-pleaded and appear to have been cut-and-pasted from an unrelated suit against Google. *See Byars*, 2023 U.S. Dist. LEXIS 24985, at *12-13 (granting motion to dismiss in similar website wiretapping lawsuit where the pleading was "replete with evidence of cut-and-paste work"). For avoidance of doubt, PSP's website is not a browser.[10] Google Chrome is a browser (though unconnected to this case), and PSP does not "render" the "Chrome Service." It sells pet supplies.

[9] 18 U.S.C. § 2510(15) usually applies to telephone and email providers. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 n.38 (2004) (citing S. Rep. No. 99-541, at 14 (1986)).

[10] "A Web browser is computer software that allows a user to view Web pages." *U.S. v. Tucker*, 305 F.3d 1193, 1197 n.4 (10th Cir. 2002).

An intended recipient of a communication is not prohibited from "divulging" the communication. Finally, any allegedly divulged communications are between Plaintiff and PSP. FAC at ¶¶ 49, 70-71, 96, 101, 270, 297. As the "addressee or intended recipient" of any purported "communications," the law permits PSP to consent to their "divulgence." *See* 18 U.S.C.S § 2511(3)(b)(2); 18 U.S.C.S. § 2702(b)(1) & (3); *see also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. May 12, 2011) ("If the communications were sent to Defendant, then Defendant was their 'addressee or intended recipient,' and thus was permitted to divulge [them]"). For these reasons, Counts VIII and X should be dismissed with prejudice.

B. Plaintiff's Device Is Not a "Stored Communications" Facility (Count IX)

An intended recipient may authorize access to its communications under the SCA. As with Counts VIII and X, the FAC identifies PSP as an intended recipient of all relevant "communications." The prohibitions of 18 U.S.C.S. § 2701 *et seq.* (on which Count IX is based) do not apply to "conduct authorized" by "a user of that service with respect to a communication of or intended for that user"). *See* 18 U.S.C.S. § 2701(c), (c)(2).

Personal devices are not electronic storage facilities within the meaning of the Stored Communications Act. Count IX asserts that Plaintiff's "devices" (her computers, mobile phones, and/or web browsers) constitute "a facility [or facilities] through which an electronic communication service is provided" and that PSP used session replay code to access and obtain information from these "facilities" without authorization. FAC at ¶¶ 285-290. There are no facts supporting these barebones recitations. Even if there were, "communications stored on personal devices are not held in electronic storage." *Cohen*, 2018 U.S. Dist. LEXIS 116372, at *14 (collecting cases). "[P]ersonal web browsers" and "personal computing devices" are not "facilities." *See Calhoun v. Google, LLC*, 526 F. Supp. 3d 605, 627-28 (N.D. Cal. 2021) (Chrome browser is not a covered facility). *Garcia v. City of Laredo*, 702 F.3d 788, 792-93 (5th Cir. 2012)

(collecting cases that distinguish "computers that *enable* the use of an electronic communication service" from "facilities," are "*operated by* electronic communication service providers and used to store and maintain electronic storage." (internal quotation marks and citation omitted)).

As any communications were intended for PSP and Plaintiff's devices are not electronic storage "facilities," Count IX fails to state a claim and should be dismissed with prejudice.

C. Plaintiff Fails to State a Claim under the CFAA (Count XI)

The private right of action at 18 U.S.C.S. § 1030(g) of the CFAA benefits those who have suffered *property damages* and incurred *remedial costs* as a result of crimes involving unauthorized access or access in excess of authority to protected computers. 18 U.S.C.S. § 1030. It offers no remedy for the speculative privacy harms Plaintiff alleges.

Failure to plead statutorily defined "damage" or "loss." The CFAA permits parties who suffer "damage or loss" to bring a civil action "if the conduct involves [at least 1 of 5] factors"[11] outlined at 18 U.S.C.S. § 1030(c)(4)(A). 18 U.S.C.S. § 1030(g). "[D]amage" "means any impairment to the integrity or availability of data, a program, a system, or information," and "loss" "means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C.S. § 1030(e)(8) & (11). *See Van Buren v. United States*, 141 S. Ct. 1648, 1659-60 (2021) (noting that these definitions contemplate "technological harms"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066-67 (N.D. Cal.

[11] The FAC seeks to allege two such factors. FAC at ¶¶ 317-318. No facts are pleaded to show any economic loss (let alone a loss from a single act amounting to $5,000) or how PSP caused a "threat to public health or safety." Plaintiff fails to substantiate either factor.

2012) (collecting authorities and dismissing CFAA claim). Plaintiff fails to allege or explain any computer harms and instead reiterates speculative privacy harms. *See* FAC at ¶¶ 317-318.

Plaintiff fails to plead a CFAA violation. In two sentences, the FAC alleges that PSP exceeded its authorized access to Plaintiff's computers and "obtained information thereby." FAC at ¶¶ 315-316. This does not substantiate an "exceeds authorized access" claim. *See Van Buren*, 141 S. Ct. at 1652 (identifying elements). In asserting that PSP "exceeded . . . authorized access" (FAC at ¶ 316), the FAC asserts a barebones legal conclusion, devoid of factual basis. Absent some explanation of PSP's authority and how that authority was exceeded, PSP cannot respond. Plaintiff's improper CFAA claim (Count XI) should be dismissed with prejudice.

VII. PLAINTIFF FAILS TO STATE CLAIMS FOR TRESPASS, CONVERSION, AND/OR REPLEVIN (COUNTS IV-VI)

Like her improperly pleaded CFAA claim, Plaintiff conflates trespass to chattels and conversion[12] with privacy torts. The essence of either claim is unauthorized use of another's property and resulting damage. *See Parziale v. HP, Inc.*, No. 19-CV-05363, 2020 U.S. Dist. LEXIS 179738, at *19-20 (N.D. Cal. Sept. 29, 2020) (dismissing trespass to chattels claim). By contrast, the gravamen of Plaintiff's pleading is that she suffered privacy injuries when she transmitted data to PSP's website. An action for trespass to chattels or conversion cannot remedy alleged "exposure" or unauthorized transmittal of data. *See* FAC at ¶¶ 217-218, 231-232. It offers

[12] All three common law property claims (Count IV, Count V, and Count VI) require substantially the same factual showing and are treated interchangeably in this Section. The common law distinction between trespass to chattels and conversion "lies in the measure of damages." Restatement (Second) of Torts § 222A cmt. c. Similarly, the distinction between replevin and conversion is the election of remedies: "Conversion is a tort against the right of possession. Replevin is a possessory action to obtain property that is in the defendant's possession." *Lafayette v. Courtney*, 189 S.W.3d 207, 210 (Mo. Ct. App. 2006) (citation omitted).

a remedy for "dispossession" of or "damage or other impairment to" *a chattel*. Restatement (Second) of Torts § 218 cmts. d & g (Am. L. Inst. 1965) (discussing remedies and damages).[13]

Plaintiff fails to plead interference with the possession, use, or enjoyment of her property. Plaintiff's common law property claims generally contend that PSP "intentionally interfered with" Plaintiff's "use and/or possession" of her "computer and/or mobile device" and the data contained therein. FAC at ¶¶ 215-216, 230-231. Like the equally skeletal CFAA claim, these claims are devoid of factual support and can be dismissed on this basis. *See Iqbal*, 556 U.S. at 678 (requiring a plausible factual showing to state a claim). The FAC does not show how PSP exercised unauthorized control or possession over something owned by Plaintiff. *See* Restatement (Second) of Torts § 217 (Am. L. Inst. 1965) (describing two ways of committing trespass to chattels); Restatement (Second) of Torts § 222A (Am. L. Inst. 1965) (defining conversion). As pleaded, the FAC shows that Plaintiff visited PSP's website and transmitted what she defines as "Website Communications," which PSP received. Receipt of intentional communications by an intended recipient is not a "dispossession." First, this information was not taken, it was transmitted by Plaintiff. And second, like a "copy of a document" or a "recipe," data describing Plaintiff's use of PSP's website cannot be "converted" (and is not subject to an action for replevin) because she "has not been deprived of possession" of anything. *See Monarch Fire Prot. Dist. v. Freedom Consulting & Auditing Servs.*, 678 F. Supp. 2d 927, 944 (E.D. Mo. 2009) (citing *Schaefer v. Spence*, 813 S.W.2d 92, 97 (Mo. Ct. App. 1991)). There is no explanation for how Plaintiff's control, enjoyment, or use of her devices was materially disturbed, and one party's receipt of information does not "dispossess" the transmitter.

[13] Missouri courts often look to the Second Restatement of Torts. *See Cover v. Phillips Pipe Line Co.*, 454 S.W.2d 507, 512 (Mo. 1970) (following Restatement (Second) of Torts § 217 in interpreting the tort of trespass to chattels).

Plaintiff fails to plead cognizable damages. Absent a claim that a defendant has literally dispossessed a plaintiff, liability for trespass to chattels lies only where any "intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected." Restatement (Second) of Torts § 218 cmt. e. If interference becomes so serious as to justify paying the full value of the chattel, the trespass becomes a conversion. Restatement (Second) of Torts § 222A(1) & cmt. c. The FAC does not demonstrate that PSP deprived Plaintiff of the use of her device or data or that the condition, quality, or value of Plaintiff's property was "impaired." *See* Restatement (Second) of Torts § 218(a)-(b); *LaCourt v. Specific Media, Inc.,* No. SACV 10-1256, 2011 U.S. Dist. LEXIS 50543, at *20-21 (C.D. Cal. Apr. 28, 2011) (dismissing trespass to chattel claim where plaintiff did not show that cookies deprived user of her device or damaged her data); *Vecchio,* 2012 U.S. Dist. LEXIS 76536, at *26-28 (dismissing trespass to chattels claim for failure to plead damages). Despite the opportunity to amend, Plaintiff's common law property claims remain threadbare recitations with no factual basis. Counts IV-VI should be dismissed with prejudice.

VIII. PLAINTIFF STILL FAILS TO ALLEGE THE BASIC ELEMENTS OF A CLAIM UNDER THE MISSOURI MERCHANDISING PRACTICES ACT (COUNT II)

Plaintiff attempts, but fails, to revive her flawed MMPA claim. In the original Complaint, Plaintiff misrepresented the text of the MMPA and failed to allege the first element of a claim: a purchase or lease of merchandise. *See generally* MMPA, Mo. Rev. Stat. §§ 407.005–.315.[14] Now

[14] The MMPA requires that Plaintiff show: (1) a purchase or lease of merchandise; (2) for personal, family, or household purposes; and (3) an ascertainable loss; (4) as a result of an unlawful act or practice. *See Hess v. Chase Manhattan Bank, USA, N.A.*, 220 S.W.3d 758, 773 (Mo. 2007).

the FAC alleges that after visiting the PSP website to search for a local pet supply store, she made an in-store birdseed purchase at some unspecified later date. FAC at ¶¶ 68, 176.

The FAC still fails to allege an "ascertainable loss" of any kind, an unlawful practice under the MMPA, or any plausible, factual nexus between the two. An ascertainable loss is a pecuniary loss, a loss of money or property. *See Grawitch v. Charter Commc'ns, Inc.*, 750 F.3d 956, 960 (8th Cir. 2014) (requiring pecuniary loss). While Plaintiff now claims that she eventually purchased something from a PSP store (birdseed), she alleges no ascertainable, pecuniary loss "thereby." *See* Mo. Rev. Stat. § 407.025.1(1). This fails to state a claim. *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 719 (8th Cir. 2017) ("to be actionable under the MMPA . . . an ascertainable pecuniary loss ***must occur in relation to the plaintiff's purchase or lease of that merchandise***.") (emphasis added). Plaintiff does not allege an ascertainable, pecuniary loss related to her birdseed purchase. She cannot show a cognizable loss caused by any practice prohibited by the MMPA. *See Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1057-58 (E.D. Mo. 2009) (dismissing MMPA claim in part for "fail[ing] to plead an ascertainable loss of money or property by reason of any unlawful practice"); *Plubell v. Merck & Co.*, 289 S.W.3d 707, 714 (Mo. Ct. App. 2009) ("[A] plaintiff's *loss* should be a result of the defendant's unlawful practice[.]"). Plaintiff cannot state a MMPA claim, and Count II should be dismissed with prejudice.

CONCLUSION

For the foregoing reasons, Defendant respectfully requests that the Court dismiss the FAC with prejudice.

Dated: February 24, 2023

Respectfully submitted,

REED SMITH LLP

/s/ Karen E. Vaysman
Karen E. Vaysman #6327730(IL)
Reed Smith LLP
10 South Wacker Drive, Suite 4000
Chicago, IL 60606-7507
Phone: 312-207-2866
Fax: 312-207-6400
Email: kvaysman@reedsmith.com

James L. Rockney #200026(PA) (*pro hac vice*)
Reed Smith LLP
225 Fifth Avenue
Pittsburgh, PA 15222
Phone: 412-288-4046
Fax: 412-288-3063
Email: jrockney@reedsmith.com

Gerard M. Stegmaier, #477145(DC) (*pro hac vice*)
Reed Smith LLP
1301 K Street, N.W.
Suite 1000, East Tower
Washington, DC 20005
Phone: 202-414-9288
Fax: 202-414-9299
Email: gstegmaier@reedsmith.com

Attorneys for Defendant PSP Group, LLC d/b/a Pet Supplies Plus

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of February 2023, a true and correct copy of the foregoing document was filed and served with the Clerk of the Court by using the CM/ECF system, which will send notification of such filing to all counsel or parties of record.

/s/ Karen E. Vaysman
Karen E. Vaysman #6327730(IL)
Attorney for Defendant